

The Browser as a Secure Platform

for Loosely Coupled, Private-Data Mashups

Ben Adida

Center for Research on Computation and Society
Harvard University

24 May 2007

web mashups: interesting combinations.

HousingMaps

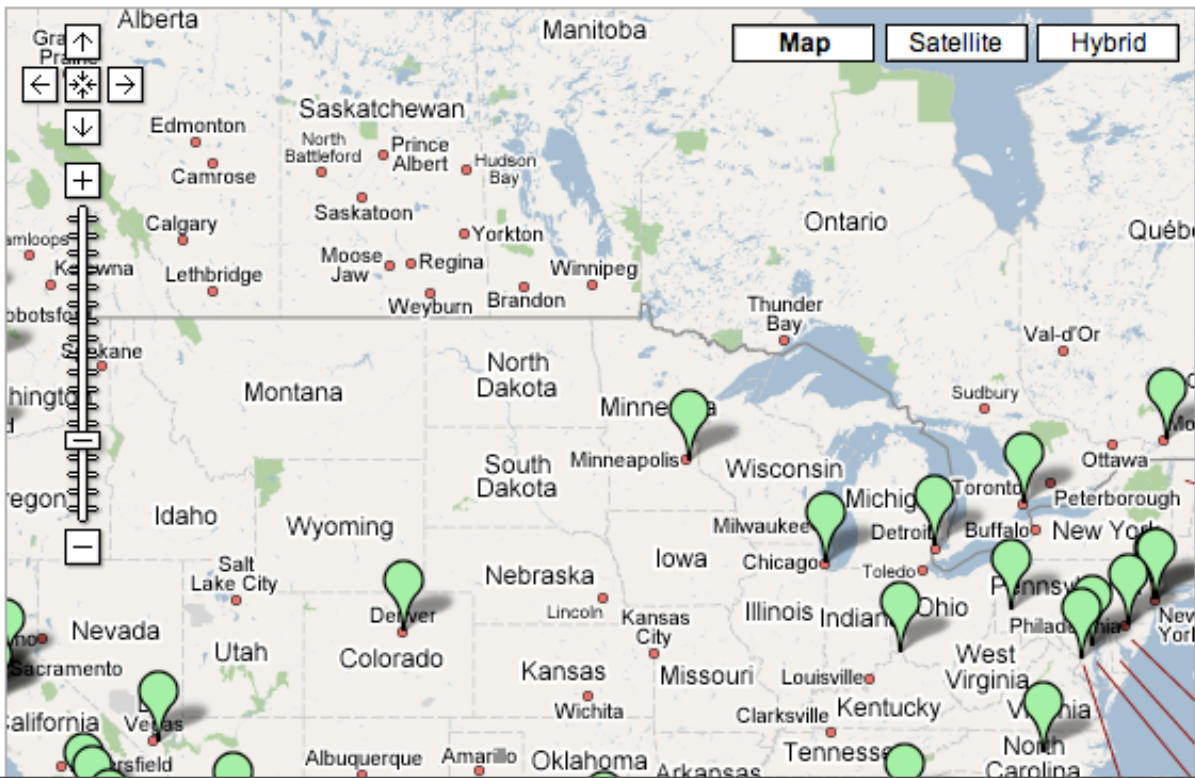
http://www.housingmaps.com/ Google

[For Rent](#) [For Sale](#) [Rooms](#) [Sublets](#)


Powered by [craigslist](#) and [Google Maps](#)
(this site is in no way affiliated with craigslist or Google) [About / Feedback](#)





City: *** Choose a city *** Price: \$1500 - \$2000 [Show Filters](#) [New](#) [Refresh](#)

Map Satellite Hybrid



Drag the map with your mouse, or double-click to center.

Click on an  icon to select a city.

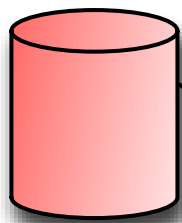
In each city, click on the  and  icons to see listings.
You can also click the  and  icons next to each listing.

Yellow icons have pictures.

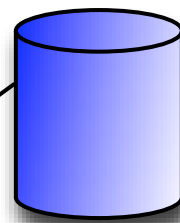
Set the price range using the drop-down menu above.

Aggressive “web 2.0”
development will continue.

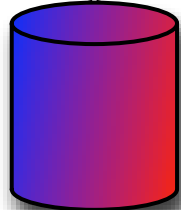
Can we make the browser
a better platform?



Service #1



Service #2



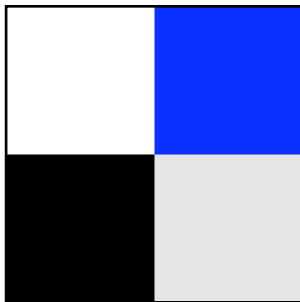
Mashup
Service

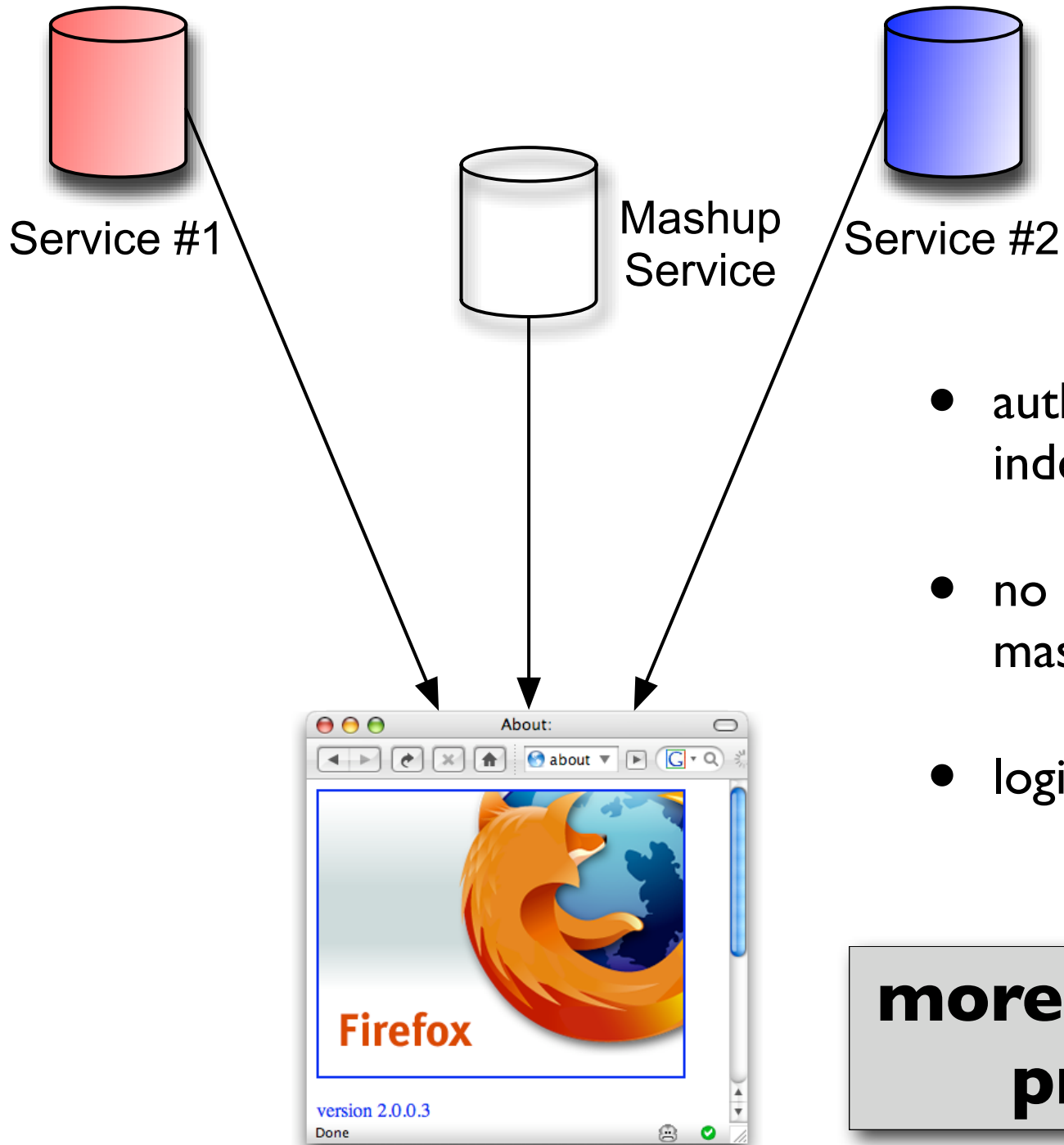


- mashup service selects which sources to combine.
- all data flows through the mashup service.
- (most of) mashup logic on the mashup server.

**great for
public data services**

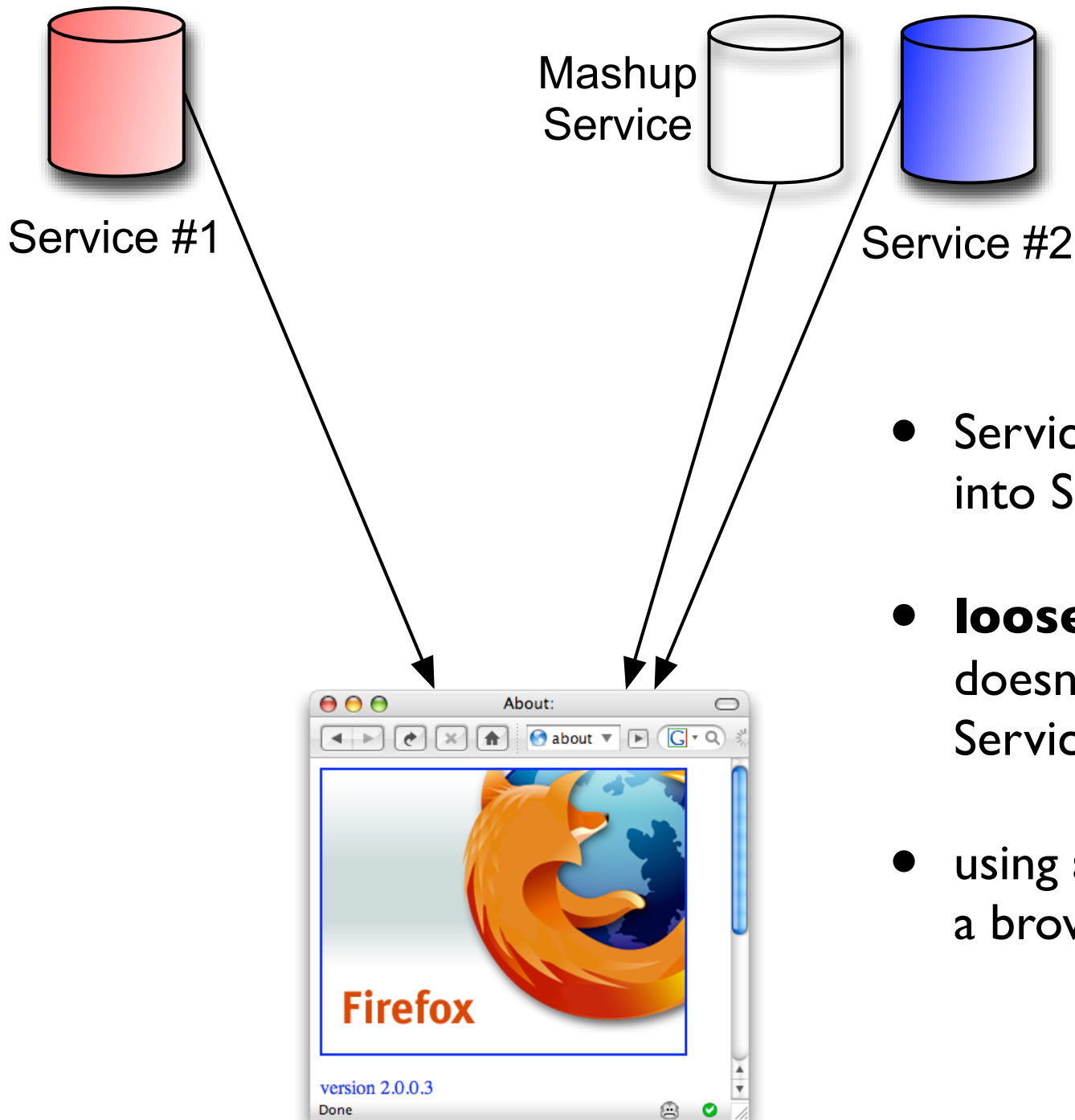
web applications increasingly manage **private** data



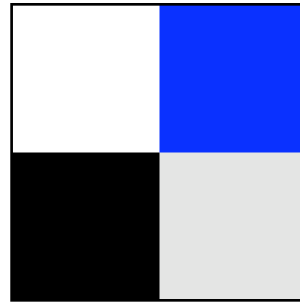


- authentication handled independently by each service
- no data flows through the mashup service
- logic runs in the browser.

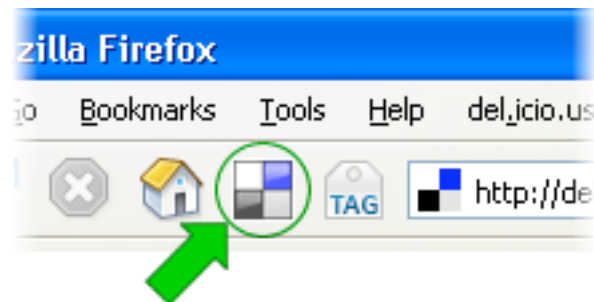
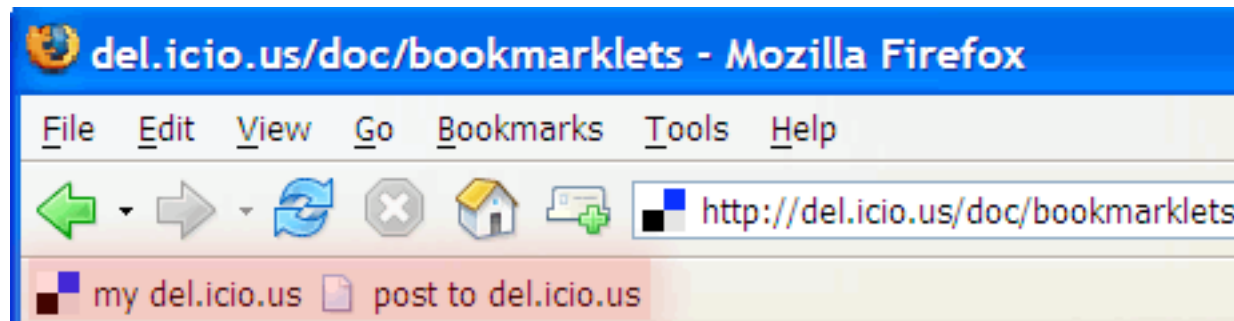
**more interesting for
private data.**



- Service #2 is “injected” into Service #1
- **loose coupling:** Service #2 doesn’t necessarily know about Service #1 ahead of time.
- using a bookmarklet or a browser extension



del.icio.us





StyleFeeder



AMERICAN MORNING SITUATION ROOM LOU DOB

Member Center: [Sign In](#) | [Register](#)

SEARCH  THE WEB  CNN.COM

Home World U.S. Weather Business Sports Analysis Politics Law Tec

UPDATED: 12:11 a.m. EDT, May 24, 2007

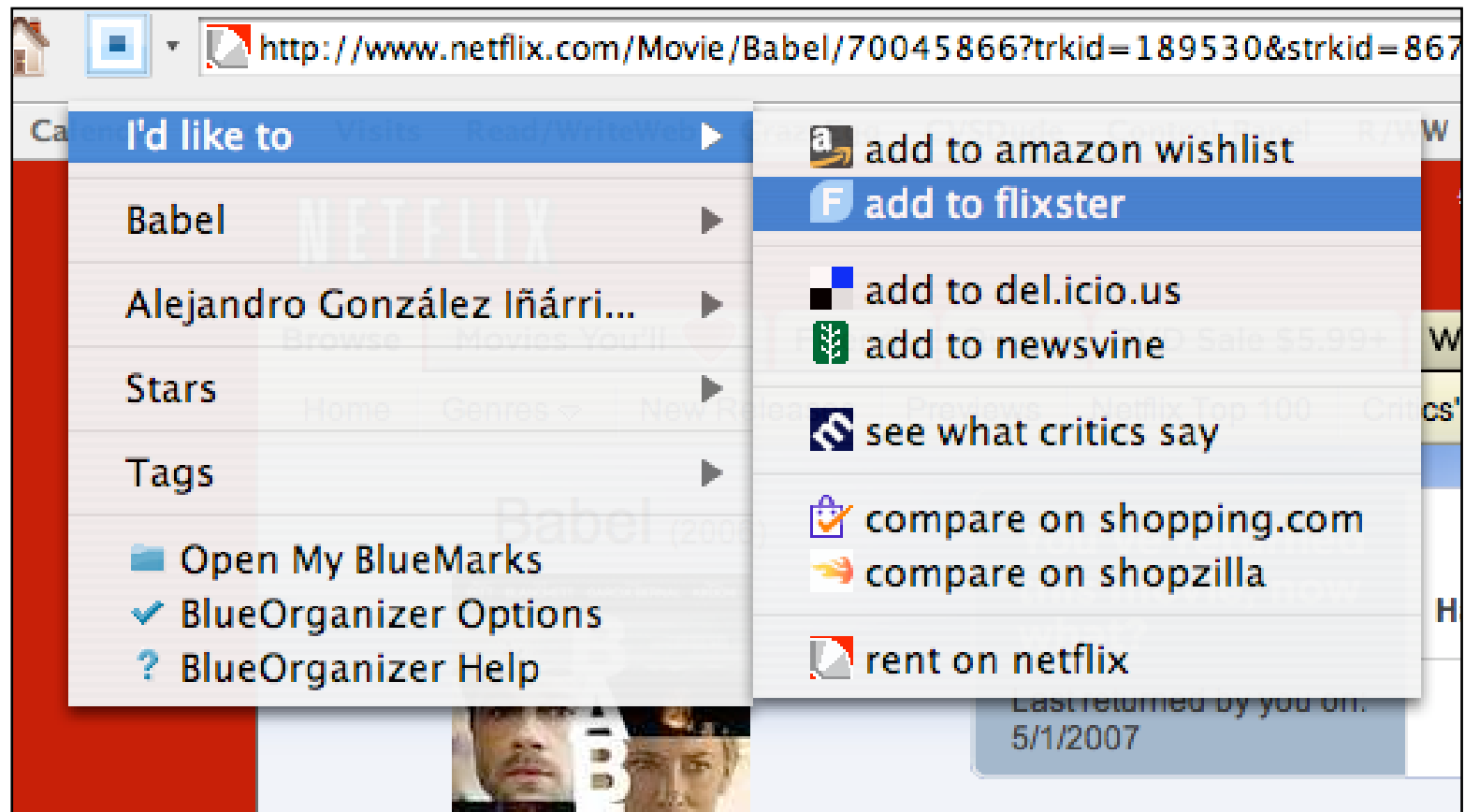


U.S. soldiers search for missing comrades.

LATEST NEWS

TOP STORIES

- [America chooses its n](#)
- [Guest worker plan sla](#)
- [ns militan](#)
- [puty's tes](#)
- [Armani, Rolex? But ba](#)
- [Two sentenced for tryi](#)
- [U.S. checking Chinese](#)
- [Shark virgin birth warn](#)
- [Spector judge: Forens](#)
- [Co-ed strips for her ho](#)
- [Oprah Winfrey 'upset'](#)



Google™ Toolbar



Google



Search



Bookmarks

Problems

- bookmarklet runs in current page's context
unstable API - bad for stability and security.
- bookmarklet limited to on-the-fly downloads
vulnerable to pharming attacks.
- extension has full control over all browsing
requires significant trust in extension!

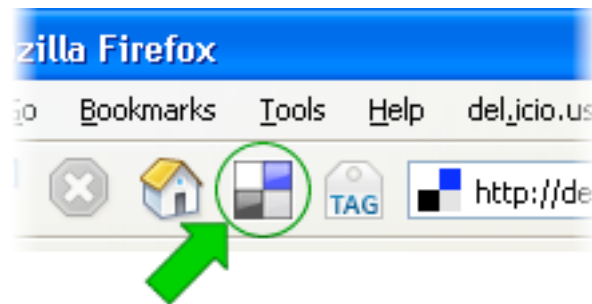
Suggested Enhancements

I. JavaScript Isolation

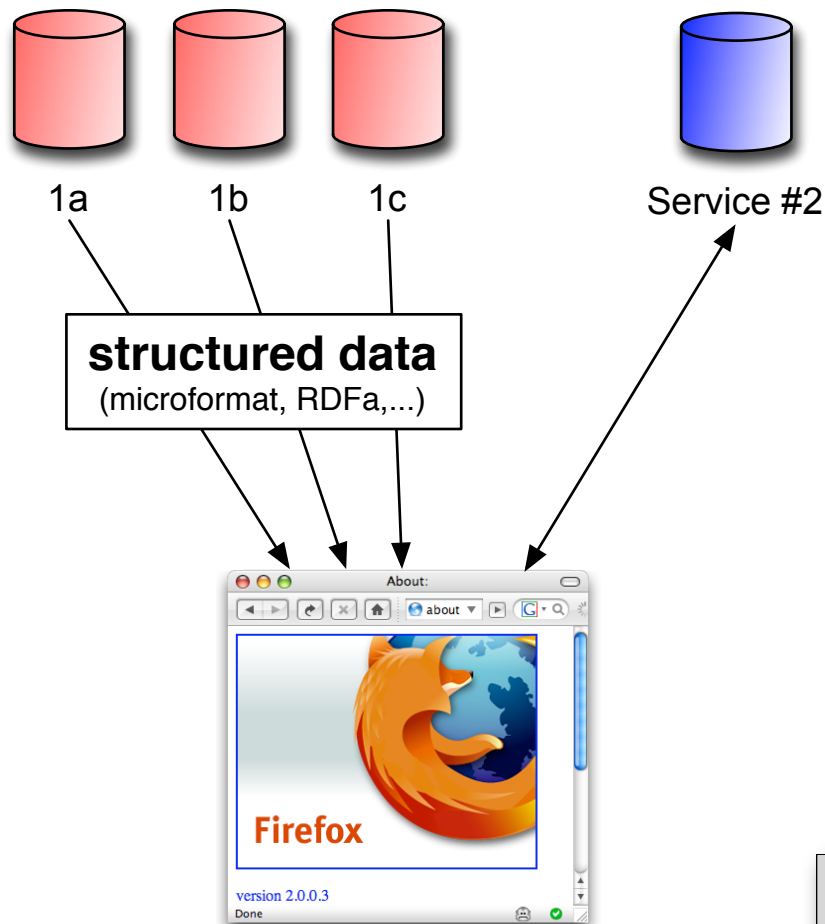
```
with_cleanslate {  
    // access DOM  
  
    // call standard JavaScript API  
  
    // ...  
}
```

2. Fine-Grained Permissions

- **Limited Awakening:** extension takes control *only* when the user invokes it.
- **Limited Network Access:** extension can access only hosts on which it is invoked.



3. Metadata-Mediated Extensions



- web services contain structured data.
- the data type triggers the appropriate extension.
- the extension can contact its own web-based service.
- (extension may not even need to contact 1a, 1b, 1c.)

**watch for the
Operator FF Extension**

Browser = Platform

- **Isolation**
- **Fine-Grained Permissions**
- **Structured Data for Inter-Application Communication**

Enhancements are backwards-compatible
with today's web



<http://flickr.com/photos/hollywoodpoodle/373053089/>

Questions?



<http://ben.adida.net/presentations/>